ITCS300 - Security and Use Standards for OPUS Employees

Scope

This document describes the basic computer security measures that must be followed by all OPUS employees; employees of OPUS subsidiaries, contractors, vendors, and others authorized by OPUS management to use OPUS internal computer systems.

This document includes two major sections: the first summarizes the most critical steps employees must take to protect personal workstations and to defend OPUS's systems against harmful code; the second summarizes employee responsibilities for protecting OPUS Confidential information, and lists security and appropriate usage requirements in a number of other circumstances that employees are likely to encounter.

Compliance Criteria

Mandatory compliance criteria are specified within the standard.

Introduction

OPUS's information and computing assets are critical to the company's success, and as a result, must be protected from loss, modification or destruction. This document describes the basic computer security measures that must be followed by all OPUS employees; employees of OPUS subsidiaries, contractors, vendors, and others authorized by OPUS management to use OPUS internal computer systems.

Note: Individuals who operate multi-user systems and applications which support OPUS production business services, Inter-Enterprise Services, local/departmental services, workstations used as kiosks, or workstations made available for general use in classrooms, visitor centers and customer briefing centers, and those supporting development processes, must also refer to ITCS104: Information Technology Security Standards for additional security control measures required for those systems and services. Please contact the HR Department if the above document is needed.

Note: Individuals who host visitors at OPUS premises are responsible for ensuring their compliance to ITCS300. If visitors wish to access into OPUS network, it is the host's responsibility to ensure explicit approval is obtained from the MIS Team.

This document includes two major sections: the first summarizes the most critical steps employees must take to protect personal workstations provided by OPUS and to defend OPUS's systems against harmful code; the second summarizes employee responsibilities for protecting OPUS Confidential information, and lists security and appropriate usage requirements in a number of other circumstances that employees are likely to encounter. Detailed instructions for implementing these requirements on particular computers and operating systems may be found in other referenced documents or from the MIS Team.

Noncompliance with the principles described in this document may result in disciplinary action, as deemed appropriate by your OPUS reporting manager.

OPUS Management will determine ITCS300 deviations necessitated by local laws and will provide appropriate guidance to the managers/employees

Document Availability:

This document and all other OPUS Security documents are available on-line in the intranet.

Document Control

This is an OPUS proprietary document. Distribution in whole or in part outside of OPUS or its subsidiaries requires the approval of the OPUS management.

This document will be reviewed annually, and will be re-issued when revisions are necessary. Obsolete copies should be destroyed as soon as practical, and shall be the responsibility of the holder

Section 1: Workstation Security Requirements

1.1 Security of your personal workstation

Every employee is responsible to help reduce the possibility and consequences of
theft of all personal OPUS computing resources and devices and the information they contain.

The following security controls must be activated on all personal workstations:

- Activate a power-on password and a hard disk password in your ThinkPad's BIOS settings.
- Activate a power-on password in your desktop workstation BIOS settings.
- Set a password protected keyboard/screen lock that is automatically activated by a period of inactivity. The inactivity time interval should be no more than 10 minutes. -

Note: You are not required to periodically change your workstation's power-on and hard disk password

Note: Desktop workstations located in Controlled Access Areas or in offices, which are locked when unattended, are not required to have power-on and keyboard/screen lock passwords applied.

1.2 When Leaving Your Office or Work Area

If you do not work in an office that can be locked:

- Activate the password protected keyboard/screen lock when you leave. (i.e., do not leave the workstation exposed for the 10-minute inactivity period required for the automated screenlock activation.)

If your notebook PC cannot otherwise be physically secured (i.e., locked in a desk drawer or filing cabinet, locked in an office, or taken with you), a cable lock must be used to secure the notebook PC to a fixed object.

Note : Cable locks can be ordered from Purchasing Department. The Kensington Master Lock is recommended

Note : If additional security controls are required, you will be notified by the MIS Team.

1.3 When Traveling or Working away from Your Office or Work Area

Keep notebook PCs in your possession if at all possible.

- When traveling by air, do not put notebook PCs in checked baggage, and be alert to the possibility of theft when going through security checkpoints at airports.
  Notebook PCs should not be left for an extended period of time in an unoccupied vehicle.
- If you must leave your notebook PC in an unoccupied vehicle, then consider securing the notebook PC to the body of the vehicle inside the trunk. Information regarding how to best secure notebook PCs in a vehicle can be obtained from the MIS Team.

If you must leave the notebook PC in a hotel, lock it in the hotel safe if one is available.

- If a safe is not available and you have a locking cable, use that mechanism.

If you are traveling with OPUS Confidential material recorded on portable media such as paper portable storage devices, work pads, notebooks, etc., you must protect this media according to the same guidelines listed above for protecting your notebook PC.

Note : If your notebook PC, or OPUS Confidential information, is stolen or lost, you must report the loss to your OPUS reporting manager.

1.4 Security of Handheld Devices

Hand held devices (tablet devices), RIM BlackBerry, smart phones with data access, etc.) require physical and logical access controls if OPUS Confidential or other business sensitive data is accessed or stored by the device. The following actions are required:

- Keep hand held devices in your possession if possible.
- Activate a power on password and a password controlled time out / lock out feature on all hand held devices supporting these security features.

1.5 Computer Viruses and other Harmful Code

Install and run an OPUS-approved AntiVirus program on your workstation.

Additional information about OPUS AntiVirus program and processes is available from the MIS Team.

- Do make sure the antivirus protection is updated periodically.

If you discover a virus, please refer to the MIS Team.

1.6 Security Firewalls

Install and run only an OPUS-approved personal firewall program on your workstation. (The current firewall program is included with the Antivirus program).

Additional information about approved firewall programs and processes is available from the MIS Team.

1.7 File sharing

You may only allow other users to access or store files on your network-connected workstation under the following conditions:

- The software that allows other users to access your files must be provided by OPUS (this is to ensure that it has been adequately checked for security holes and legal and licensing restrictions).

Note: The use of Internet-based peer-to-peer file sharing services, such as bit torrent, on OPUS workstations is prohibited.

- You must not allow anonymous FTP, TFTP, unauthenticated HTTP, or other unauthenticated access to areas of your hard disk that are also used for other purposes. For instance, you may not "share out" your entire hard drive with anonymous access.
- You must not allow any form of unauthenticated access to data or programs that are classified OPUS Confidential, or to areas of your hard disk that may contain such data or programs.
- If it is necessary to allow access to areas of your hard disk that are also used for other purposes (for instance, to allow remote maintenance or update of components of the operating system), or to OPUS Confidential materials, you must select either userid access control or password access control when defining the share options and the access must be granted only to the limited list of people with a need for that access (not, for instance, to anyone who authenticates with an OPUS intranet password).

For advice on how to configure your system to share files securely, refer to the MIS Team.

Section 2: General Security & Use Requirements

2.1 OPUS Management Approved Use of Computer Services

Please refer to **OPUS' Business Conduct Guidelines**

2.1.1 Personal Use of Computing Equipment

Please refer to **OPUS' Business Conduct Guidelines**

2.1.2 Chain letters, Hoaxes and Virus Warnings

Please refer to **ITCS300 FAQ**

2.1.3 Offensive and Inappropriate Material

Please refer to **OPUS' Business Conduct Guidelines**

2.1.4 Web Cameras

Please refer to **OPUS' Business Conduct Guidelines**

2.2 Legal Considerations

2.2.1 Software Licenses

Please refer to **OPUS' Business Conduct Guidelines**

2.2.2 Copyright and Intellectual Property

Most information and software (programs, audio, video, data files, etc.) that is available in the public domain (including on the Internet) is subject to copyright or other intellectual property right protection. When obtaining material for use inside OPUS:

- Do not obtain software from such sources for use within OPUS unless express permission to do so is stated by the material owner.
- You must read and understand any software copyright restrictions. If you think that OPUS will not be able to comply with any part of the terms, do not download or use the material.
- Ensure that you comply with any expressed requirements or limitations attached to the use of such software (for example: not to be used for commercial purposes; can not charge others for use or distribution; subject to a copyright or attribution notice being affixed to each copy; must distribute source code; etc.).
- If you are unsure about the meaning of the restrictive language or have questions about it, you should contact an OPUS attorney to review it before downloading or using the material.
- You must obtain assistance and approval from OPUS Legal or Intellectual Property Law counsel before incorporating any public domain material into a product or material OPUS intends to distribute externally.

2.2.3 Privacy (Data Protection) Legislation

Please refer to **OPUS' Business Conduct Guidelines**

2.2.4 Protecting Another Company's Classified Information

Please refer to **OPUS' Business Conduct Guidelines**

2.2.5 Releasing OPUS Information into the Public Domain

Seek advice from OPUS Intellectual Property Law counsel before uploading any OPUS software to the Internet. You must ensure that any OPUS copyright documents clearly indicate OPUS as holder of the copyright.

2.3 Protecting OPUS Information

2.3.1 Passwords

The password associated with a computer access userid is the primary means of verifying your identity, and subsequently allowing you access to the computer and to OPUS information. For your own protection, and for the protection of OPUS' resources, you must keep your identity verification password secret and not share it with anyone else.

Note: The power-on and hard disk passwords you use to help protect against unauthorized access to your workstation are not identity verification passwords. These passwords are not associated with your identity, but rather, can be managed like doorlock keys or safe combinations. It is not a violation of security policy for you to notify your OPUS reporting manager of these passwords.

NOTE: Recent changes to information protection and data privacy laws in various countries include specific requirements for the selection of secure identity verification passwords, and compliance with these password rules is a legal obligation. The OPUS password rules listed below are consistent with current international requirements.

Identity verification passwords must not be trivial or predictable, and must:

- Be at least 8 positions in length
- Contain a mix of alphabetic and non-alphabetic characters (numbers, punctuation or special characters) or a mix of at least two types of non-alphabetic characters **.**
- Not contain your userid as part of the password

OPUS internal business systems and applications containing OPUS Confidential information require you to change your password at least once every six months (180 days). In cases where the system or application does not use technical control measures to force you to change your password, it is your responsibility to comply with the password change requirement. When changing your password, you must select a new password, i.e., do not change the password to one that you used in the past.

Note: If you access computer systems that are not under OPUS control, do not select the same password on external systems that you selected for use on OPUS internal systems.

2.3.3 Protecting OPUS Confidential Information

The primary requirement for protecting OPUS Confidential information is that it must be protected from access or viewing except by people who have a business need to know the information.

OPUS requires the encryption of OPUS Confidential information when it is sent over the Internet, public networks, or wireless devices. Refer to the MIS Team for additional information about encryption tools.

When you store OPUS Confidential information on computer systems (e.g. group web sites, or other shared data repositories), you must use software security controls to manage and limit access to the information. Security controls must never be set to allow unrestricted access (e.g., Worldreadable, "public") to OPUS Confidential information. If you do not understand how to correctly set or use the security controls, you should ask for advice or assistance from the MIS Team.

When you store OPUS Confidential information on mobile storage media such as but not limited to, tapes, compact disks (CDs), removable storage device, etc., you must protect the information against theft and unauthorized access. Label the media OPUS Confidential and keep them in a locked area or storage device when they are not in use. Never leave them exposed in unattended areas.

Do not store or process OPUS Confidential information on systems that are not controlled by you or OPUS.
Do not enter OPUS Confidential information on Internet web sites that offer translation services, e.g. yahoo babel fish
When printing OPUS Confidential information you must protect the information against theft and unauthorized viewing. (The term "printer" includes printers, plotters, and any other device used to create hard copy output.) OPUS Confidential information may only be printed: in a controlled access area, with access based on "need to know", or; in an attended OPUS printer facility, where the output is given only to its owner, or; on a printer with capture/release facility that you control, or; on a printer that you are personally attending, or; if Printing Systems Manager (PSM), or an equivalent function, is available in the location where you are working, use it to control printing. For additional information, refer to the MIS Team . If none of these options are available at your location, you may use a printer located within an open area in OPUS internal office space, but you must pick up your OPUS Confidential printout material within 10 minutes.

2.3.4 Using Telephones, Facsimile (FAX)

Please refer **ITCS300 FAQ**

2.3.5 Using Teleconferencing Systems

When chairing an OPUS Confidential teleconference, confirm that all participants are authorized to participate, before starting any discussion.

2.4 OPUS/Customer's Internal Networks

When connected to and using OPUS internal networks, including Local Area Networks (LANs):

- Do not misrepresent yourself (i.e., masquerade) as someone else on the network.
- Do not monitor network traffic (i.e., use a "sniffer" or similar device) without first obtaining explicit management approval and permission from the MIS Team.
- Do not run security testing tools/programs against any Intranet system or server, other than those that you directly control, without first obtaining explicit management approval.

- Do not add any network device that extends the OPUS infrastructure (e.g. devices or devices functioning as: Switches, Bridges, Routers, Hubs, modems, wireless access points, etc) for any reason without first obtaining permission from the MIS Team.
- You are not to connect to a Customer's internal network unless you are explicitly authorized to do so. If you are authorized to connect to their network, it is your responsibility to ensure that your workstation is configured to access their network as per Customer's instructions or requirements.

2.5 External Connections and Remote Access

Please refer to **ITCS300 FAQ**

2.6 The Internet

2.6.1 Conduct

Please refer to **ITCS300 FAQ**

2.6.2 Receiving Unsolicited e-mail

Please refer to **ITCS300 FAQ**

2.6.3 Privacy

Please refer to **ITCS300 FAQ**

Section 3: Security Incident Reporting

If you suspect a security incident is in progress or has occurred, it is important for you to act promptly by contacting your OPUS Reporting Manager.

- Employees are *not* to attempt to investigate or take action against the offender unless directed to do so by your OPUS Reporting Manager.

If you have security questions, discuss them with your OPUS reporting manager or the MIS Team.

Contact Information for IT Department

MIS Support Hotline	: 6427 8644